CLAIMS:

We claim:

1. A method for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the method comprising the steps of:

soliciting a secured connection with a reverse proxy protecting a back-end server computing device;

establishing a connection with said back-end server computing device via said reverse proxy through said solicitation; and,

responsive to establishing said connection, maintaining said connection and exchanging non-HTTP data over said secured connection without encapsulating said non-HTTP data within HTTP messages.

2. The method of claim 1, wherein said soliciting step comprises the step of requesting a secured sockets layer (SSL) connection with said reverse proxy.

3. The method of claim 2, wherein said requesting step comprises the steps of:

acquiring an address for said reverse proxy and a port for establishing an SSL connection with said reverse proxy;

further acquiring an address for said back-end server computing device and a port for establishing an SSL connection with said back-end server computing device;

formulating an HTTP-CONNECT message using said acquired addresses and ports; and,

writing said formulated HTTP-CONNECT message to said reverse proxy.

4. The method of claim 1, wherein said exchanging step comprises the steps of:

formatting a buffer with real-time data; and,

writing said buffer to said secured connection.

5. The method of claim 1, further comprising the step of performing authentication in said reverse proxy as a condition of establishing said secured connection.

6. A system for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the system comprising:

a reverse proxy disposed between a client computing device and a server computing device in a computer communications network;

an authentication process configured for operation in conjunction with said reverse proxy;

a communications socket established between said reverse proxy and said client computing device; and,

a non-HTTP data handler coupled to said secured communications socket and programmed to write non-HTTP data to said reverse proxy without encapsulating said non-HTTP data within HTTP messages.

7. The system of claim 6, wherein server computing device is a real-time streaming media server, said non-HTTP data handler is a real-time streaming media client, and said non-HTTP data is real-time streaming media.

8. The system of claim 6, wherein said communications socket is a secured sockets layer (SSL) communications link.

9. A machine readable storage having stored thereon a computer program for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the computer program comprising a routine set of instructions for causing the machine to perform the steps of:

soliciting a secured connection with a reverse proxy protecting a back-end server computing device;

establishing a connection with said back-end server computing device via said reverse proxy through said solicitation; and,

responsive to establishing said connection, maintaining said connection and exchanging non-HTTP data over said secured connection without encapsulating said non-HTTP data within HTTP messages.

10. The machine readable storage of claim 9, wherein said soliciting step comprises the step of requesting a secured sockets layer (SSL) connection with said reverse proxy.

11. The machine readable storage of claim 10, wherein said requesting step comprises the steps of:

acquiring an address for said reverse proxy and a port for establishing an SSL connection with said reverse proxy;

further acquiring an address for said back-end server computing device and a port for establishing an SSL connection with said back-end server computing device;

formulating an HTTP-CONNECT message using said acquired address and port; and,

writing said formulated HTTP-CONNECT message to said reverse proxy.

12. The machine readable storage of claim 9, wherein said exchanging step comprises the steps of:

formatting a buffer with real-time data; and,

writing said buffer to said secured connection.

13. The machine readable storage of claim 9, further comprising the step of performing authentication in said reverse proxy as a condition of establishing said secured connection.